4. Implementation Twofish Algorithm for Data Security in a Communication Network Using Library Chilkat Encryption ActivEx

by Much Aziz Muslim

Submission date: 23-Jul-2019 01:15PM (UTC+0700)
Submission ID: 1154275073
File name: mmunication_Network_Using_Library_Chilkat_Encryption_ActivEx.pdf (630.92K)
Word count: 2804
Character count: 16170

Journal of Theoretical and Applied Information Technology
29th February 2016. Vol.84. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

IMPLEMENTATION TWOFISH ALGORITHM FOR DATA SECURITY IN A COMMUNICATION NETWORK USING LIBRARY CHILKAT ENCRYPTION ACTIVEX

[1]MUCH AZIZ MUSLIM, [2]BUDI PRASETIYO, [3]ALAMSYAH

[1,2,3]Department of Computer Science, Semarang State University, Indonesia
Email: [1]a212muslim@yahoo.com, [2]budipras@mail.unnes.ac.id, [3]alamsyah@mail.unnes.ac.id

ABSTRACT

Cryptography is required to secure the data networks communication. This study implements Twofish cryptographic algorithm using library Chilkat Encryption ActiveX Ms. Visual Basic. Twofish operate on a block of plaintext consisting of 128 bits. There are 3 steps in Twofish algorithm, the first step is divide input bit into 4 parts, the second step was performed XOR operation between bit input with a key, and the third step processing the input bits in 16 times Feistel network. To facilitate the implementation of the coding in Ms. Visual Basic we use Chilkat Encryption ActiveX. This research using agile methods with phases: plan, design, code, test, and release. Twofish algorithm implementation using Ms. Visual Basic and library Chilkat Encryption ActiveX can be used to secure the data. The data succeed to be encrypted or decrypted and irreversible. The program can be implemented to maintain the confidentiality of the data when transmitted over the Internet. The speed encryption process need 3 times longer than the decryption. Average of time in encryption process need 0,365 second, while decryption process need 0,0936 second.

Keywords: *Data security, Twofish, Chilkat Encryption ActiveX*

1. INTRODUCTION

Along with the times, the human need for information is increasing. Halfway in the development of information technology is increasingly lively, internet no longer guarantee the provision of secure information [1]. Various search-engine continues to grow along with mushroomed viruses, bugs, spam and hackers that can steal confidential data [2].

Security and confidentiality problem is one of data and information important aspects. Therefore, delivery and storage of data via electronic media requires a process that ensures security and integrity of the data. Thus, we need a way to secure data and information in other forms, namely encoding-decryption process (encryption). Encryption is done when the data will be sent. This process will transform an original data into confidential data which cannot be read. Meanwhile, decryption process done by the data receiver. Received confidential data is converted back to the original data using a key.

Various ways being developed to improve data security, including cryptography. Cryptography is done by randomizing messages so it cannot be read [3]. With this encoding method, the original data will not be read by unauthorized parties. There are several algorithms in cryptography for data encryption. Improveing security in hardware network has been implemented using DES [4].

NIST makes Advanced Encryption Standard (AES) as the new standard. One of AES candidate is Twofish algorithm created by Bruce Schneier. Twofish meets all the criteria needed by NIST, 128-bit block, 128 bit, 192 bit and 256 bit keys. Some advantages of Twofish namely Twofish is a 128-bit block cipher that receives the keys with variable length of 256 bit, Twofish does not contain weak keys, and Twofish has been designed from the beginning with the emphasis on the performance [5]. Based on the description above, it is necessary to do research on the process of Twofish algorithms encryption and their implementation in computer program of Ms. Visual Basic with Chilkat Encryption ActiveX.

2. REVIEW OF LITERATURE

2.1. Cryptography

Cryptography is derived from two Greek words, namely "Crypto" which means secret, and "graphy" means writing. In maintaining the

Journal of Theoretical and Applied Information Technology
29th February 2016. Vol.84. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

confidentiality of the data, cryptography transforms clear data (plaintext) into the form of password data (ciphertext) which cannot be recognized. Cryptography is a science that studies mathematical techniques related to information security aspects, such as data confidentiality, data authenticity, data integrity, and authentication of data [6]. Encryption of Cryptography as in Figure 1.

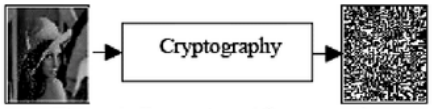

Figure 1: Encryption of Cryptography

Cryptographic system or cryptosystem is a facility to convert plaintext into ciphertext and vice versa. Cryptography basically consists of two processes namely encryption process and decryption process. Encryption process is encoding process of an open message into a secret message (ciphertext). Afterwards, the ciphertext will be delivered through a channel of an open communication. At the time the ciphertext is received by the message receiver, then the secret message changed again into open message through decryption process so that the message can be read back by the message receiver. In general, the process of encryption and decryption can be drawn as follows.

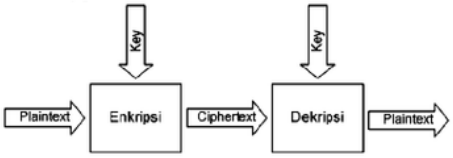

Figure 2: The process of encryption and decryption [7]

2.2. Twofish Algorithm

Twofish algorithm is a strong algorithm that until now declared safe because there is still no crypt analysis attacks which can really break it. This algorithm is also not patented so its use on encryption tools does not need cost. Twofish algorithm is one of the algorithms which is recommended as AES. It is due to the fulfillment of design criteria by NIST as standard of AES namely:

1) 128-bit symmetric cipher block
2) Having key lengths among others: 128 bit, 192 bit, and 256 bit.
3) There is no weak keys
4) Having the efficiency on the software and hardware from different platforms.
5) Having a flexible design, for example, receive an additional key length, can be applied to software and hardware from different plat form, suitable for stream cipher, hash function and MAC.
6) The design is simple in order to facilitate the process of analysis and implementation of algorithms.

In addition to the criteria mentioned above, it also added the performance criteria on Twofish as follows [8]:

1) Accept any key lengths up to 256 bit.
2) Encrypt the data in less than 500 clock cycles per block on Intel Pentium, Pentium Pro and Pentium II, for a fully optimized version of the algorithm.
3) Able to form 128-bit key (for optimal encryption speed) in a time less than the time required to encrypt 32 blocks on Pentium, Pentium Pro and Pentium II.
4) Does not use operations that make Twofish inefficient on microprocessor except 32-bit, 8 bit microprocessor and 16 bit microprocessor.

2.3. Visual Basic

Visual Basic is a programming language products issued by Ms., one of the leading software companies in the world. Visual Basic is a programming language that is easy to use for the development of system, either a small system or big system. With many controls componets provided by Visual Basic, making programmers and system developers are easier in the manufacture of the system. Visual Basic is widely used by programmers and system developers, because of the convenience offered. In the system development, the programmer is not too troubled by the look of the program, because Visual Basic provides plenty of control components to design the look of the program. Visual Basic can develop various types of systems, such as database systems, internet networks, multimedia graphics, and others.

2.4. Chilkat Encryption ActiveX Reference

Chilkat Encryption ActiveX is a component which separated from Ms. Visual Basic. Chilkat Encryption ActiveX used to add controls such as encryption and decryption, one of which is for encryption and decryption with DES algorithm. By using Chilkat Encryption ActiveX Reference very ease users to create applications that are

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

inserted encryption and decryption with DES algorithm in Ms. Visual Basic 6.0.

3. METHOD

3.1. Research Method

Solving a problem begins with the development of software in the process of combining steganography and cryptography used Agile method as seen in Figure 3. Agile methods used to software development, for example for the development of expert systems [9]. Agile methods can be used for the development of other systems. In this study, we use Agile methods.

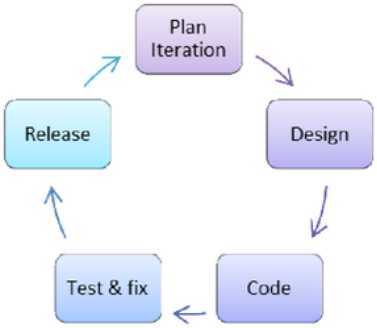

Figure 3. Research Method of Agile

Agile method is a particular approach to project management that is utilized in software development. Agile method used to develop software based on short-term development system that require adaptation rapidly than the developer to changes of any form [10].

1) Plan

At this stage, needs analysis carried out literature studies and the collection of information about the process which will be used to construct models of cryptography including:

a. Software requirement analysis.
b. Twofish algorithm.
c. Data security.

2) Design

Designing is a process of translating system according to the algorithms used. It intends that the program made in accordance with the results of needs analysis. The result of this step is interface design as shown in Figure 4.

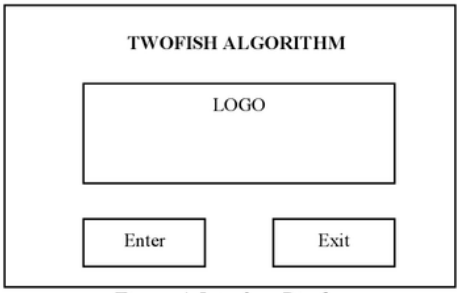

Figure 4. Interface Display

Interface of the program consists of a logo and 2 buttons menu namely Enter menu which used to enter the program and Exit menu to exit from the program.

3) Code

Coding stage is a stage of translating program design which has been made into commands form which is understood by computer. In this research, it is conducted writing of program code in accordance with the design step by using Visual Basic software. In the encoding also made the system interface to facilitate interaction between the users program.

4) Test

In this study, the test program is done by giving input with some kinds of cases that might be found. Input which used for testing in this study is in the form of text data as secret message. The test methods used in this software is blackbox testing method, which focuses on the functional requirements of software [11].

3.2. Twofish Algorithm Structure

Twofish operate on a block of plaintext, which consists of 128 bits. Twofish block diagram as shown in Figure 5.

Journal of Theoretical and Applied Information Technology
29th February 2016. Vol.84. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

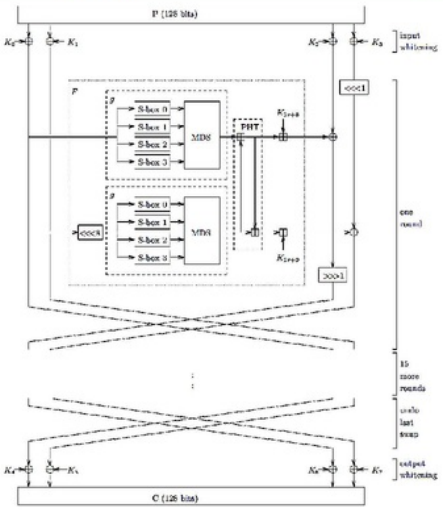

Figure 5: Twofish algorithm structure

In the Twofish algorithm implementation, there are several things that must be considered [5], including:

1. Bit input as much as 128 bits would be divided into four sections, each for 32 bits using little-endian convention. Two parts of the bit will be the right part, the two parts of the other bits will be left.
2. Bit-XOR input in advance with the four key parts (whitening).

$$R_{0,i}=P \oplus K_i;\ i=0,\ldots,3 \qquad (1)$$

Where K is the key, K_i means the sub key where i=0, ...,3.

3. Twofish algorithm uses a Feistel network structure. Feistel network used by Twofish consists of 16 iterations. Function f of Twofish consists of several stages:
   a. Function g, which consists of four s-box and MDS matrix
   b. IPM (pseudo-Hadamard transform)
   c. The addition of the key results of IPM.

4. RESULTS AND DISCUSSIONS

The result of this implementation was a data security system application using Twofish algorithms that was built with Ms. Visual Basic 6.0. On the interface directly displayed inputs of encryption and decryption. This system divided into two processes, namely the encryption process which had function to convert plaintext into ciphertext and decryption process which had function to change ciphertext into plaintext. Interface display of Twofish implementation showed in Figure 6.

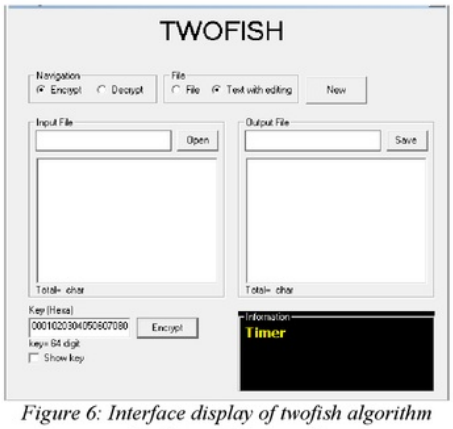

Figure 6: Interface display of twofish algorithm implementation result

1) Encryption Process

The encryption process was a process of open message change which could be read (plaintext) into information that we could not be understood its contents (ciphertext). In this system, the writer used Twofish cryptographic algorithms to perform the encryption process. Plaintext would be encrypted into the information / message which could not be understood. The program code of encryption process as follows:

```
    crypt.CryptAlgorithm = "Twofish"
    crypt.CipherMode = "cbc"
    crypt.KeyLength = 256
    crypt.PaddingScheme = 0

    crypt.EncodingMode = "hex"

    Dim ivHex As String
    ivHex =
    "000102030405060708090A0B0C0D0E0F"
    crypt.SetEncodedIV ivHex, "hex"

    Dim keyHex As String
    'keyHex = "0001020304050607"
    keyHex = Text3.Text
    'crypt.SetEncodedKey keyHex, "hex"
    'keyHex =
"000102030405060708090A0B0C0D0E0F10111213141516
1718191A1B1C1D1E1F"
    crypt.SetEncodedKey keyHex, "hex"
    Dim encStr As String
        encStr =
crypt.EncryptStringENC(Text4.Text)
        'MsgBox encStr
        Text1.Text = encStr & vbCrLf
        Text9.Text = encStr
```

Journal of Theoretical and Applied Information Technology
29th February 2016. Vol.84. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Results of the program which have been made then tested to perform the encryption process as follows.

a. Input plaintext:
Twofish was a cryptographic algorithm that operated in a block cipher mode sized 128-bit with a key sized 256 bit. A large key size is intended to obviate the possibility of weak key. Twofish algorithm was a development of Blowfish algorithm.

b. Input the key (hexa):
000102030405060708090A0B0C0D0E0F10111213141
5161718191A1B1C1D1E1F

c. Doing the encryption process. Encryption Result as follows:
E0307C4BA359C337BA2FD54EEE9B07F27DA308509D
1A06D3C7867B13E9D46A9F6753BD4698AE3BE667F9
A6A574A26C9C8BB9D04AB8C57AB96E94F216E58FC9
7EB6AD50C27A68EE2796823AFCD7840ADBDB864879
92B86C850373893DBA4595D8D0155ED56E1B28A506B
42E53AA8538A23D0D168ECB5F2FD8FC540255B68868
374B8EE6BAD31F413F16D5F539D426624E7039E7591
3735F0531809BCEE6554A0B99DB57FCD91ED9473E84
452D77DECA0AE070FADE5482390468862C44DE6E79
DFBBB7BCB6558B29B47BFE9DA4F4906C612B5A3F4B
AE7FA227C629BF4A6EE7DDA50FD8A59CA26F6460D1
6696EFC822992BB8005B0E1DFF1384ACFA0F19711FD
2AE

Interface display of encryption process showed in Figure 7.

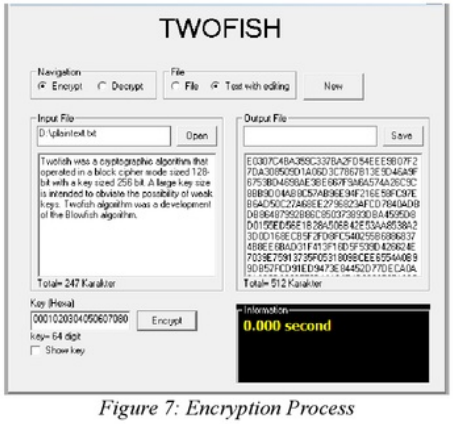

Figure 7: Encryption Process

2) Decryption Process

Decryption was the process of returning ciphertext file into plaintext file. Thus, in general, decryption process was the reverse of encryption process. Ciphertext would be decrypted by using DES algorithm. The program code of encryption process as follows.

```
'Decrypt
Dim decStr As String
    decStr =
crypt.DecryptStringENC(Text9.Text)
    Text4.Text = decStr & vbCrLf
```

Result of the program have been made and then tested to perform the encryption process as follows.

a. Input chipertext:
E0307C4BA359C337BA2FD54EEE9B07F27DA308509D
1A06D3C7867B13E9D46A9F6753BD4698AE3BE667F9
A6A574A26C9C8BB9D04AB8C57AB96E94F216E58FC9
7EB6AD50C27A68EE2796823AFCD7840ADBDB864879
92B86C850373893DBA4595D8D0155ED56E1B28A506B
42E53AA8538A23D0D168ECB5F2FD8FC540255B68868
374B8EE6BAD31F413F16D5F539D426624E7039E7591
3735F0531809BCEE6554A0B99DB57FCD91ED9473E84
452D77DECA0AE070FADE5482390468862C44DE6E79
DFBBB7BCB6558B29B47BFE9DA4F4906C612B5A3F4B
AE7FA227C629BF4A6EE7DDA50FD8A59CA26F6460D1
6696EFC822992BB8005B0E1DFF1384ACFA0F19711FD
2AE

b. Input the key (hexa):
000102030405060708090A0B0C0D0E0F10111213141
5161718191A1B1C1D1E1F

c. Doing the decryption process. Decryption result as follows:
Twofish was a cryptographic algorithm that operated in a block cipher mode sized 128-bit with a key sized 256 bit. A large key size is intended to obviate the possibility of weak keys. Twofish algorithm was a development of the Blowfish algorithm.

Interface display of decryption process as showed on Figure 8.

Figure 8: Decryption Process

Further analysis of the speed of program execution process. The data used are the test results using a program that has been created with the computer specifications Core-i3. Researchers tested encryption and decryption of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the file with a different size. Further analysis of the test results as follows.

Table 1. Speed of program execution process

Filename	File size	Time (s)	
		Encrypt	Decrypt
100.txt	100Kb	0,093	0,031
200.txt	200 Kb	0,234	0,047
300.txt	300 Kb	0,312	0,078
400.txt	400 Kb	0,421	0,125
500.txt	500 Kb	0,765	0,187

Speed of execution process shown in Figure 9.

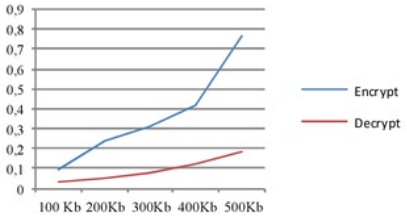

Figure 9: Speed of execution process

5. CONCLUSION

Twofish operates on a block of plaintext, which consists of 128 bit. The stage of data security uses Twofish algorithms including encryption and decryption. Twofish algorithm implementation using Ms. Visual Basic and library Chilkat Encryption ActiveX can be used to secure the data. The data succeed to be encrypted or decrypted and irreversible. The program can be implemented to maintain the confidentiality of the data when transmitted over the Internet.

REFERENCES:

[1] Adeyinka, O. 2008. Internet Attack Methods and Internet Security Technology. *Second Asia International Conference on Modelling and Simulation*, pp.77-82, 13-15 May 2008.

[2] Kautzar, M.G. 2007. *Studi Kriptografi Mengenai Triple DES dan AES*. ITB. Bandung.

[3] Schneier, B. 1996. Applied Cryptography 2nd Edition. Wiley & Sons. Inc., New York.

[4] Kantham, L., Ravi, S. 2014. Enhancing Data Security Using DES with Hardware Implementation. *Journal of Theoretical and Applied Information Technology (JATIT)*, May 2014, Vol. 63 No. 2.

[5] Schneier, Bruce, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson. 1998 "*Twofish : A 128-bit block chiper*".

[6] Menezes A.J., Oorschot, P.C., and Vanstone, S.A. 1996. *Handbook of Applied Cryptography*, CRC Press, Boca Raton, New York.

[7] Munir, R. 2006. Pengantar Kriptografi. ITB, Bandung.

[8] Hassouna, M. 2013. An End to End Secure Mail System Based on Certificateless Cryptography in the Standard Security Model. *International Journal of Computer Science Issues (IJCSI);* Mar2013, Vol. 10 Issue 2.

[9] Muslim, M.A., Kurniawati, I., Sugiharti, E., 2015. Expert System Diagnosis Chronic Kidney Disease Based on Mamdani Fuzzy Inference System. *Journal of Theoretical and Applied Informations Technology (JATIT),* Vol. 78 No. 1.

[10] Gandomani, T.J., H. Zulzalil, A.Z.A. Ghani & A.A.MD. Sultan. 2013. Important Considerations For Agile Software Development Methods Governance. *Journal of Theoretical and Applied Informations Technology (JATIT),* Vol. 55 No. 3.

[11] Pressman, R.S., 2001, Software Engineering: A Practitioner's Approach, 6th Edition, The McGraw-Hill Companies, Inc, Singapore.

4. Implementation Twofish Algorithm for Data Security in a Communication Network Using Library Chilkat Encryption ActivEx

ORIGINALITY REPORT

7%	%	7%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Dewi Soyusiawaty, Anna Hendri Soleliza Jones, Panggah Widiandana. "Similarity Detection of Student Assignments Using Rocchio Method", 2018 12th International Conference on Telecommunication Systems, Services, and Applications (TSSA), 2018 Publication	3%
2	Gayathri A., P. Narayanasamy. "Security in MANET's by Using Detective Signature Techniques", Journal of Computer Science, 2015 Publication	2%
3	Budi Triandi, Evri Ekadiansyah, Ratih Puspasari, Lili Tanti Iwan, Fitrianto Rahmad. "Improve Security Algorithm Cryptography Vigenere Cipher Using Chaos Functions", 2018 6th International Conference on Cyber and IT Service Management (CITSM), 2018 Publication	1%
	"Selected Areas in Cryptography", Springer	

4 Nature, 1999
Publication

1%

Exclude quotes	On	Exclude matches	< 10 words
Exclude bibliography	On		